Novel Schemes For Authentication

Vikash Kumar Gupta

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Odisha, India

Novel Schemes for Authentication

Thesis submitted in

partial fulfillment of the requirements

for the degree of

Bachelor of Technology

in

Computer Science and Engineering

by

Vikash Kumar Gupta

[Roll: 109CS0592]

under the guidance of

Prof. S K Jena

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Odisha, India

Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, India. www.nitrkl.ac.in

Prof. S K Jena
Professor

May 13, 2013

Certificate

This is to certify that the work in the thesis entitled ***Novel Schemes for Authentication*** by ***Vikash Kumar Gupta*** is a record of an original research work carried out under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Computer Science and Engineering.

To the best of my knowledge, the matter embodied in the thesis has not been submitted for any degree or academic award elsewhere.

Prof S K Jena

Acknowledgment

I take this opportunity to express my profound gratitude and deep regards to my guide Dr. S. K. Jena for his exemplary guidance, monitoring and constant encouragement throughout the course of this project. The blessings, help and guidance given by him time to time shall carry me a long way in the journey of life on which I am about to embark.

I am obliged to all the professors of the Department of Computer Science and Engineering, NIT Rourkela for instilling in me the basic knowledge about the field that greatly benefitted me while carrying out the project and achieving the goal.

Also, I am highly indebted to Mr. Santosh Sahoo Sir, Department of Computer Science and Engineering, National Institute of Technology, Rourkela who invested his full effort in helping me in finalizing this project within the limited time frame and keep motivated me all the time.

Lastly, I am grateful to my friends, for their relentless support in augmenting the value of work; my family, for being considerate and appreciative throughout; and Almighty, for everything.

Vikash Kumar Gupta

Abstract

Authentication is one of the most basic process to provide security to any resource and application from unauthorized access. It covers two security goals confidentiality and integrity. Passwords are used as private identity for an individual. The password also has to be protected from several threats like stealing, shoulder surfing, eavesdropping and guessing.

The most common method used for user Authentication is textual password using alphanumeric usernames and alphanumeric passwords. The issues which should be kept in mind while choosing a password is the how strong the password is and how good it is to memorize. Sometimes the stronger passwords are not easier to remember and easier passwords are not so secure. One more criteria for a good password, that should satisfy is, the password should be easy to type, such that any intruder, if any, is there beside you should not be able guess it or any camera behind you can't capture the actual movements.

To overcome the drawbacks of traditional textual schemes the new methods like graphical passwords are used. The easiness in remembering them and a strong resistance towards the brute force and dictionary attacks made them more popular. In this project, we have concentrated to protect our password from the above threats and to develop a system which has a strong resistant to above stated threats. We have implemented a varying password scheme which provides a better resistant to shoulder surfing, eavesdropping and guessing. This is an untraditional approach to use a not very complex and not very strong password in unsafe environments like public places. One more concern about the password security is to be resistant against keystroke dynamics. To overcome this we have implemented the virtual keyboard and to make it more effective we are using multilingual keys.

And also a hybrid system is designed by mixing three schemes: textual passwords, Recognition based passwords and Recall based password. All three are working together to remove the drawbacks of each scheme.

Contents

List of Figures

Chapter 1

Introduction

1.1 Authentication

Authentication is the process of confirming and validating the truth of an attribute or entity. It is an act of determining whether an individual should be allowed or not to access a system or an application. It ensures two basic goals of security: integrity and confidentiality. It is the very effective and first line of method to ensure security against the unauthorized access to any resource or to any application. The level of security for different application are different, thus the acceptability of any authentication scheme depends on its robustness against attacks as well as its resource requirements. For ex, a "chat server" needs less sophisticated approach of authentication compared to accessing the corporate database.

1.1.1 Types of Authentication Systems

The several types of schemes for authentication can be categorized as [1]:

- **What you know** Includes traditional textual password based schemes or the PIN based schemes.
- **What you have** Includes Authentication by smartcards or electronic tokens.
- **What you are** Includes the schemes like biometric authentication systems.

The most common type of schemes is "what you know". And, among them the most common scheme we use is textual password i.e. using alphanumeric username and passwords. They are simple to use and simple to implement. For less sophisticated authenticity they can be used. We can choose a strong password to provide stronger security but more strong passwords leads to more complexity. And, more complex passwords are difficult to memorize and which leads individual to write them down on the paper that can be stolen so there is a compromise to security. One more criteria for a good textual password is that it should be easy and quick to type and are not vulnerable against key stroke dynamics. Textual based schemes have many problems like shoulder surfing, key logger, vulnerable to guessing, dictionary attack and hard to remember [1].

"What you have type of scheme includes the smartcards and electronic tokens. Token based system count on the use of physical device suck as electronic key and smart cards for authentication [1]. Token based systems are vulnerable man in middle attacks where an attacker captures the users session and archives the authorizations by acting as a proxy between the individual and the authentication system without knowledge of the user [1].

"What you have" type of schemes includes the biometric authentication systems. They relies on the features of an human which remains unchanged during all his lifetime like DNA Sequence, signature, voice, retinal pattern and fingerprint etc. The main problem of this type of scheme is their high cost. The devices needed for identification process are highly costly. These types of schemes are also vulnerable to replay attack.

Textual Passwords

They are simple to use and simple to implement. For less sophisticated authenticity they can be used. We can choose a strong password to provide stronger security but more strong passwords leads to more complexity. And, more complex passwords are difficult to memorize and which leads individual to write them down on the paper

that can be stolen so there is a compromise to security. One more criteria for a good textual password is that it should be easy and quick to type and are not vulnerable against key stroke dynamics. Textual based schemes have many problems like shoulder surfing, key logger, vulnerable to guessing, dictionary attack and hard to remember [1].

Graphical-Based Password Techniques

There are many problems with the textual passwords. Like, the attacker can have idea about the password by key stroke dynamics like by looking and monitoring the movements of users hands on the keyboard. It is the fact that pictures are easy to remember than text [2]. So we can create a better password scheme which will be easy to remember for the user so password will be safe from stealing. And moreover the graphical scheme provides better security against some common type of attacks like brute force attacks, dictionary attacks and etc. The major problem they have that they are easily targeted by shoulder surfing.

Graphical Password Schemes are categorized into two categories:

Recognition based In this schemes, users are displayed a group of images and for authentication the user have to click on the correct images, for more security the ordering of the selection of images can also be used. A study told that user can remember his graphical password with 90% accuracy, even after two or three months. The recognition based scheme is vulnerable to mouse tracking and replaying.

Recall based In this type of scheme, the users are asked to reproduce something that he had been created during the registration phase. For example, a user selects a pattern during registration procedure and he has to remember that pattern and on entering that patter he will be able to access the desired application or resource. This scheme is mostly used in mobiles.

1.2 Attacks on Passwords

For authentication an individual need a private identification for the authenticity, for these private identifications we use Passwords. There are several threats to passwords, which are listed below:

- Brute force Attack
- Dictionary Attack
- Guessing
- Eavesdropping
- Shoulder Surfing
- Accessing the password file
- Stealing the password

1.3 Literature Review

1.3.1 Varying Password Based Scheme

To protect password from shoulder surfing and eavesdropping, Mohammad Shahid and Mohammad A Qadeer discussed the scheme which is motivated by the Unix System in which password of unlimited length can be typed, but only eight characters are significant [3] and salting. To secure textual password, in this scheme the password will be the part of the input string and along with that during registration the user will mention the starting position and length of the password.

For example if we choose our password abcd, and staring position 4, then the possible input string can be 123**abcd**3fofvn, xyz**abcd**dchjk.

The problem with this scheme is that it can easily be breakable by simply XOR operation. And for this scheme user have to remember the starting position and be careful about the starting position.

1.3.2 Graphical Password

To improve some shortcomings of textual passwords, graphical passwords provide some better alternatives to some problem, but they are vulnerable to shoulder surfing. Many authors have proposed many schemes for improvement.

Ahmad Almulhem [4], proposed a hybrid authentication system of graphical and textual password. The proposed authentication system is as follows. During registration, user generates a graphical password by first selecting an image and then selecting several point-of-interests (POI) in the picture. Each POI is described by a circle with the clicked point as center and some specified area around center [4]. After that POIs are associated with word or phrases. At the time of login user will select the point in the picture and then will enter the corresponding word in password textbox. If the selected points and also the corresponding word or phrase matches with the stored data, the authentication will be success.

Haichang Chao and Xiyang Liu, also proposed a login system which in implemented in a gaming way to make login process more interesting. In this scheme, image background color is used as security factor.

Sadiq Almuairfi, Prakash Veeranraghavan and Naveen Chilamkurti[1] proposed an image based implicit authentication system. This scheme says that there will be several images, each image will have several click points and each click point will be associated with several attributes. During registration, the user will provide some information and from that information some keywords will be abstracted. At the time of authentication, the server may choose a random keyword associated to the user and choose a random image that has the text attribute related with the object and sends to the users [1]. The individual has to select the correct object that signifies the expected keyword [1]. This scheme also suffers from shoulder surfing. Though we have achieved the security against dictionary attack and brute force attack, but shoulder surfing will be still there.

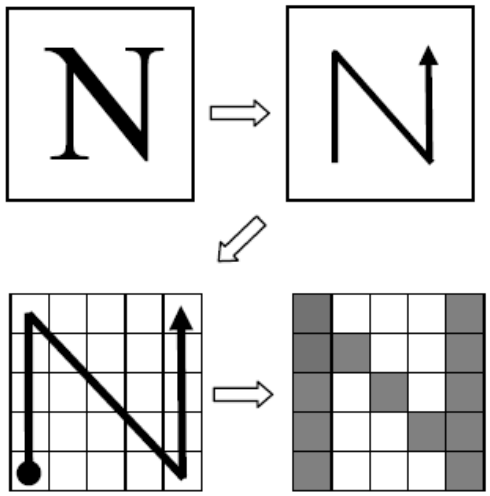

Figure 1.1: Registration Process for Stroke Based Authentication System

Ziran Zheng, Xiyu Liu, Zhaocheng Liu and Lizi Yin[5], have proposed a recall based password authentication system with textual password. In this scheme, during registration user will be shown a grid and he has to select a pattern and then according to pattern select the grid points as in shown fig 1.1 [5]. Then the pattern and order is stored. During Authentication process user have to enter the passwords by traditional input devices in some text area, according to the values shown in the grid. If the values entered in the text area matches with the values at grid point in correct order, as shown in fig 1.2 [5], then the authentication will be successful. The order of the selection of points in the pattern can be in any manner. So this scheme provides better security. During authentication the grid will shows the values 0 or 1, which are randomly generated every time. The use of 0,1 will provide ambiguity which in turn will be good against the shoulder surfing. The text area is used to enter the input password to provide more resistant to shoulder surfing.

This scheme provides a much better resistance to the shoulder surfing and brute force attack by providing a new interface every time. Though this is a time consuming approach but can be used for more secure applications.

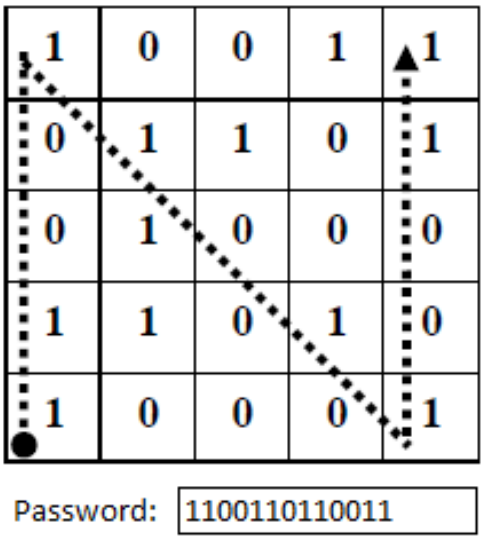

Figure 1.2: Authentication Process for Stroke Based Authentication System

1.4 Motivation

We have seen various methods like textual Passwords and Graphical Passwords. In textual password, the main problem is that maximum time user has to choose such a password which is easy to remember and provide a desired level of security according the need by the application or the resource. So if password is more complex then user needs to write them down in some paper they can be go to wrong hand. And if they are simple then they are easy for guessing and can easily be attacked by dictionary attack and brute force attack.

To secure textual password, the previous existed scheme which was motivated by the salting uses the substring method. The password will be the part of the input string and along with that during registration the user will mention the starting position and length of the password. But as it has fixed starting position, it is not so effective, though it is better for shoulder surfing than simple scheme, but if attacker get two input string, by simply doing XOR he can obtain the password. This can be stronger if the user is free to put the password at any position in the input string.

Graphical passwords which are better than textual schemes against dictionary attacks and brute force attacks, but they are weaker against shoulder surfing because

mouse movements can easily be tracked by any camera behind the individual and can be simply observed by the attacker.

So, we can use the hybrid scheme, which extracts both the features of textual password and graphical password.

The previously existing scheme which uses the combination of both, the recall based graphical password and textual password. But though it provides better resistance to shoulder surfing, but the pattern selected is static. So we can make it stronger by choosing the pattern dynamically.

1.5 Objective and Scope of the Work

The project is carried out with the following objectives:

- To study the various Authentication schemes and analyze them based on security parameters and types of attacks
- To develop Novel scheme for protecting passwords, especially to protect against shoulder surfing, guessing and eavesdropping.
- To develop a Novel and Hybrid Authentication Scheme for User Authenticity.

We have improved "varying password scheme [3] for protection of passwords against eavesdropping, shoulder surfing. And we have also developed a Hybrid scheme for authentication using combination of Recall based Graphical Password; Recognition based Graphical Password and Textual password. All the schemes have some merits and demerits. In our approach we are using the feature of one scheme to improve the feature of another scheme mutually.

1.6 Outline of Thesis

The thesis consist of four chapters following this chapter:

Chapter 2: Varying Password Based Scheme

In this chapter we have discussed an improvement in the varying password scheme and their implementation, working and analysis.

Chapter 3: Multilingual Virtual Keyboard

In this chapter we have designed a virtual multilingual keyboard with Indian Languages like hindi, odiya and Telgu.

Chapter 4: Hybrid Authentication Scheme

In this chapter we have suggested a hybrid scheme which uses property of Textual passwords, recognition based graphical Passwords and Recall based Graphical Password and their analysis.

Chapter 5: Conclusion

Here we have concluded the main points of the thesis..

Chapter 2

Varying Password Based Scheme

2.1 About the Scheme

The scheme is motivated by the scheme discussed by the Mohammad Shahid and Mohammad A Qadeer. In their scheme they were using the password as the substring of the input string, but in their scheme they were fixing the starting position of the string in the input string and also storing the length of the password. The starting position was predefined at the time of authentication by the user [3]. But this scheme can easily be break by simply XOR operation of two input string. And user has to remember the starting position as well.

So, motivated by this scheme, we have improved this scheme, which is better than this scheme. We are doing this, by just removing the restriction of choosing the fixed starting position. The password string can be anywhere in the input string. For example if our password is abcd, then the input string can be 123abcd19jfdjdfj, 1234djabcdfdruoi, abcd1234589 or 1234344abcd. The password can be anywhere in the string.

2.2 Implementation

This looks like a single substring matching algorithm. But the problem was that, the passwords are stored in the password files by using some one way trapdoor function. And the hash value of the stored passwords and the input string will be totally

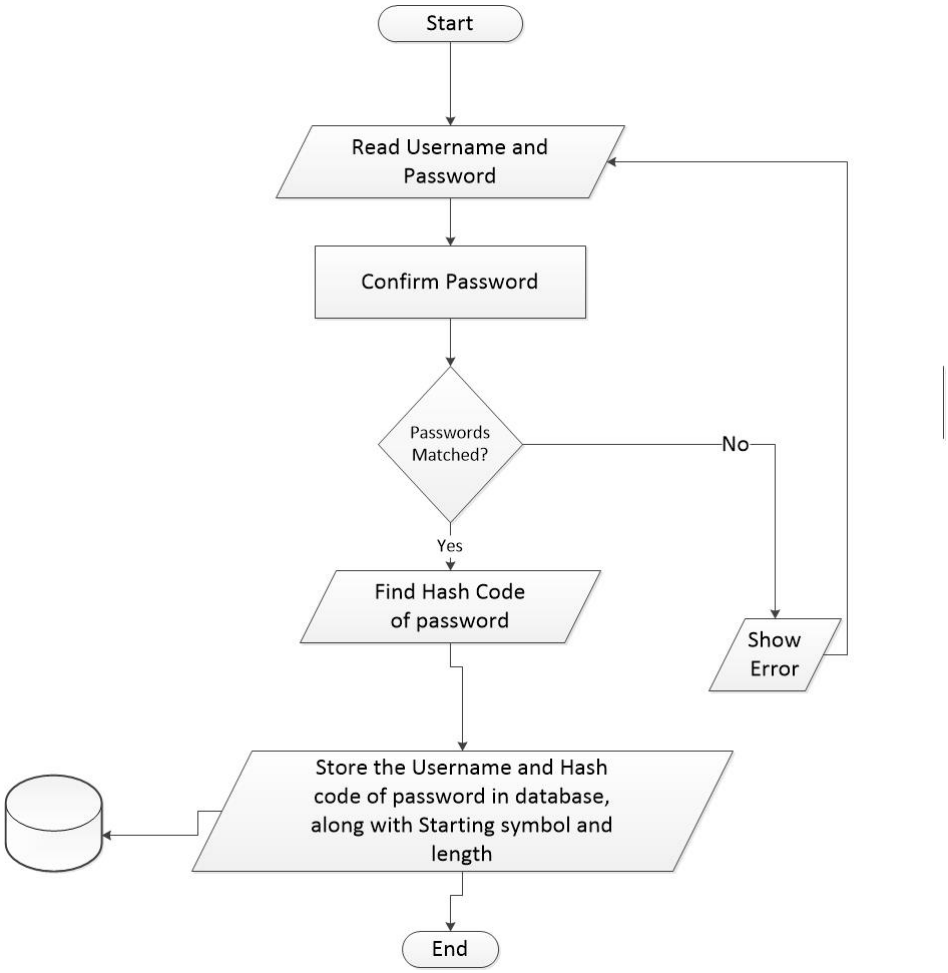

Figure 2.1: Registration Process: Varying Password Scheme

different. So, at the time of registration with it we are storing the information of starting symbol, like the hash value of start symbol of password, and length of password, as shown in fig 2.1 At the time of Authentication, we follow the following algorithm shown in fig 2.2.

2.2.1 Registration Process

2.3 Analysis of the above scheme

2.3.1 X-OR Attack

- In old scheme the actual password can be guessed of detected using XOR operation, if two input password is known. 123**abcd**aawwww Xyx**abcd**fifffif

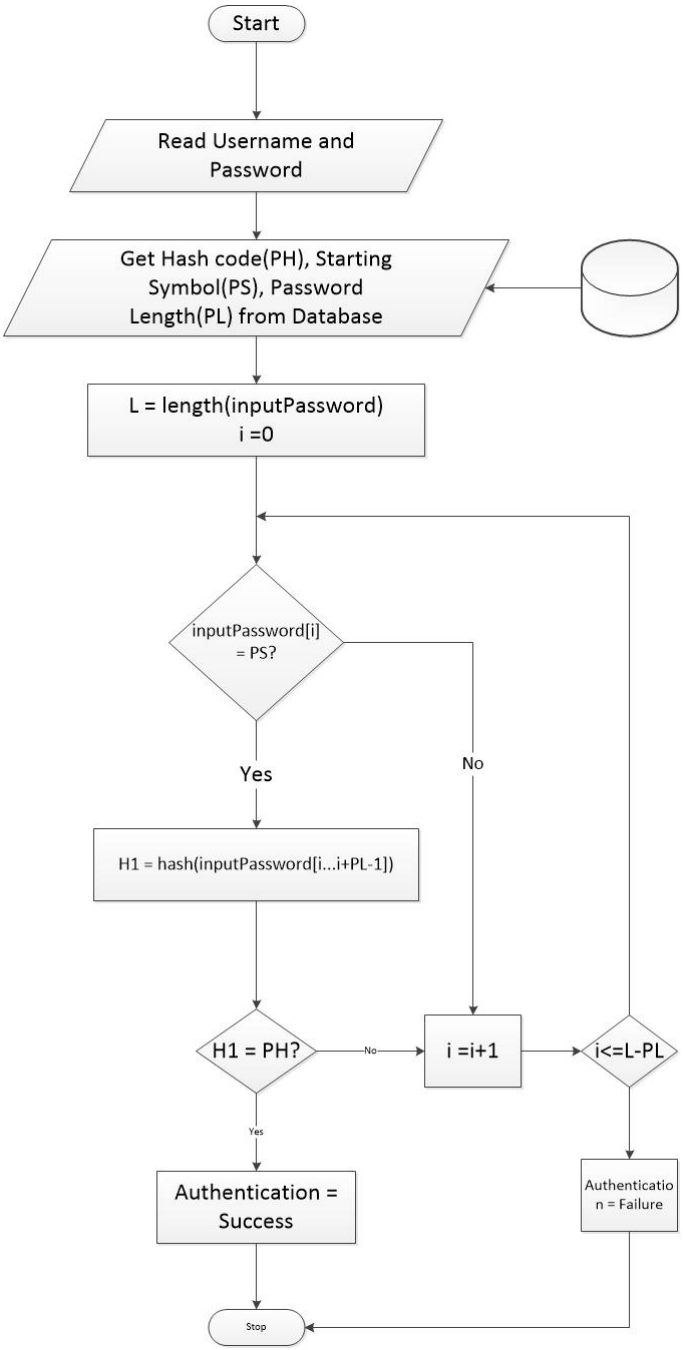

Figure 2.2: Authentication Process: Varying Password Scheme

- But in our scheme, the password can be anywhere in the input string. So provides resistance to XOR operation. 123**abc**dfsk 12344**abcd**wik

2.3.2 Eavesdropping

The password is hidden in a string, so it is not easy to see the password when user type. So, the small passwords can also be used effectively. For ex. xyz is easier to observe and remember but auenxyzejs is not so as the password is of varying length so provides better security against eavesdropping. Also during transmission from client to server machine, if someone tries to intercept it or use the traffic analysis method than due to dummies password characters in password as prefix and suffix will avoid it.

2.3.3 Shoulder Surfing

The input string will be of arbitrary length. The length of the password will be new every time. And uses of prefixes and suffixes will increase the resistance against shoulder surfing.

2.3.4 Guessing

The attacker can guess by seeing the length or by checking some common keywords or phrases. In our scheme input password string will be of varying length and of varying characters, so it will not be easy for the attacker to guess the password. And also, we can use some small random passwords and can be effectively used to avoid guessing.

2.3.5 Stealing the Password

The more complex passwords are difficult to remember, so sometimes user writes them down on some paper. This way the password can be stolen from the user. So it is better user choose a password which is easy to remember. In our scheme, we can have a password which is easy to remember, a long known phrase or somewhat not so long but with random keys which are easy to remember. To increase the security

our method makes the password complex by giving the virtue to add some dummies characters as suffix and prefix.

2.3.6 Other Advantages

- No need to remember the starting point.
- If any error occurred during the giving the password, no need to go back, we can just start giving the password again, as the password can appear anywhere in the string.
- The small password can be effectively used against the shoulder surfing.

2.4 Drawback

The time complexity of the Authentication process will increase as there will not be single matching, we have to calculate the Hash code of many strings which have equal length as original password, and have starting character whose hash value is matches with the starting character of the password.

2.5 Application

At Public Places If we are using our password at some Public places, then this scheme provide a better resistance against eavesdropping and shoulder surfing.

Chapter 3

Multi- Lingual Virtual Keyboard

3.1 Multilingual Virtual Keyboard

Virtual keyboards are the software components which allows user to enter the characters. The main advantage of using virtual keyboard is it reduces the threat of keystroke logging. By using virtual keyboard we can make the key pattern dynamic and also can use multilingual characters to provide more security. But along with this they have some disadvantages too. They have the risk of disclosure of password via shoulder surfing. Another disadvantage is that a user may not be able to "point and click" as fast as they could type on a keyboard, thus making it easier for the observer. To make the virtual keyboard more effective we can randomize the positions of the keys of the virtual keyboard every time. We can also use multilingual characters and symbols in virtual keyboard to make it more effective against eavesdropping. The multilingual keyboard can be implemented using Unicode. The Unicode is a computing industry standard for consistent encoding.

3.2 Implementation

We have implemented virtual keyboard in Visual Studio using C#. And we have implemented the virtual keyboard in many Indian languages like Hindi, Odiya, Bengali and Telgu. Figure 3.1 shows the virtual keyboard in English. Figure 3.2 is showing virtual keyboard in Hindi Language. Figure 3.3 shows the virtual keyboard in Odiya

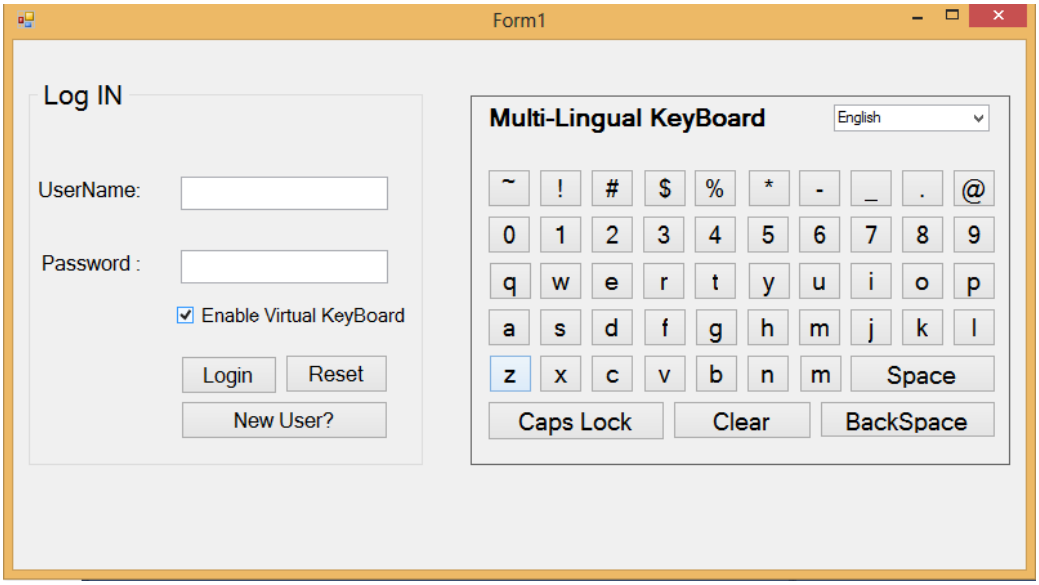

Figure 3.1: Virtual Keyboard - English

and figure 3.4 shows the virtual keyboard in Telgu.

3.3 Analysis

3.3.1 Brute Force Attack

Using the multilingual keyboard sufficiently reduces the brute force attacks. We are using multilingual keyboard, so we have character set of 260 characters. The analysis is shown through the figure 3.5

So we can see that using multilingual virtual keys we can avoid the brute force attack.

3.3.2 Eavesdropping

Using local languages in the keys can avoid eavesdropping to a significant extent. If the intruder is not known to the individuals mother language, then it will be very difficult to observe him, even if the intruder will type slowly. He cant even remember that.

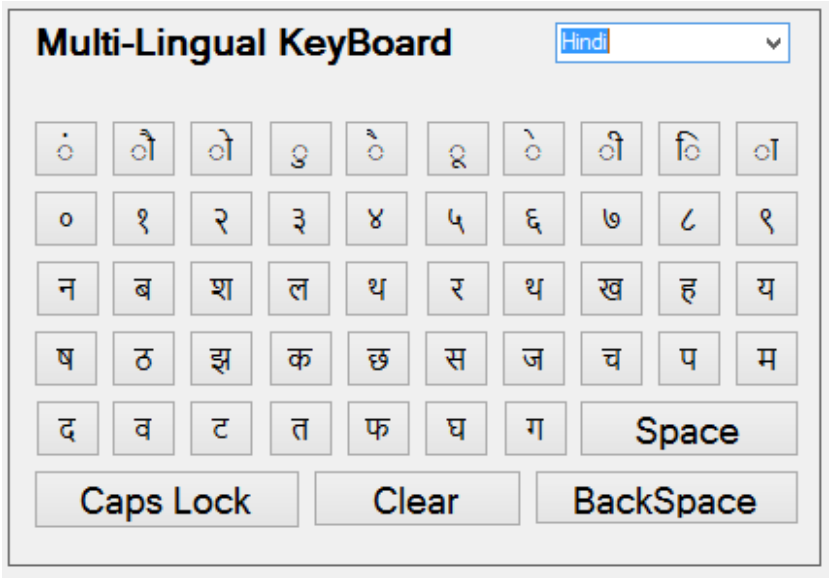

Figure 3.2: Virtual Keyboard - Hindi

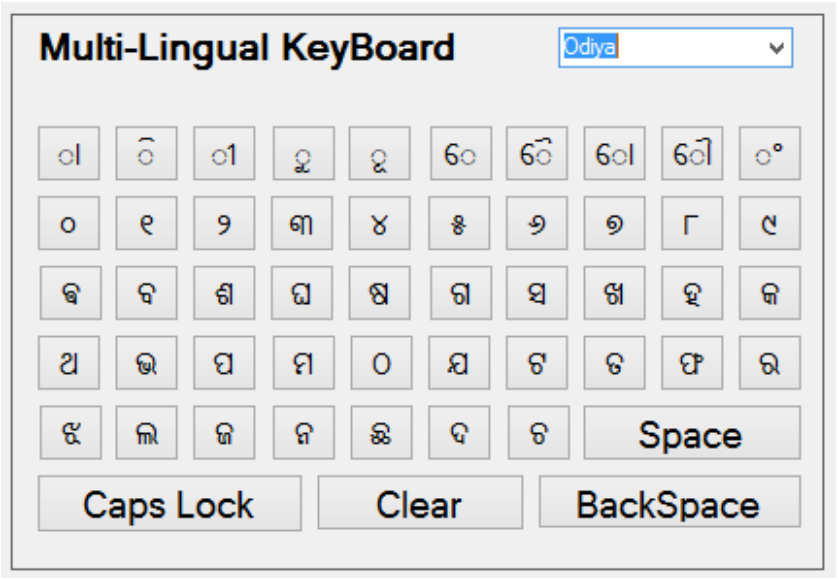

Figure 3.3: Virtual Keyboard - Odiya

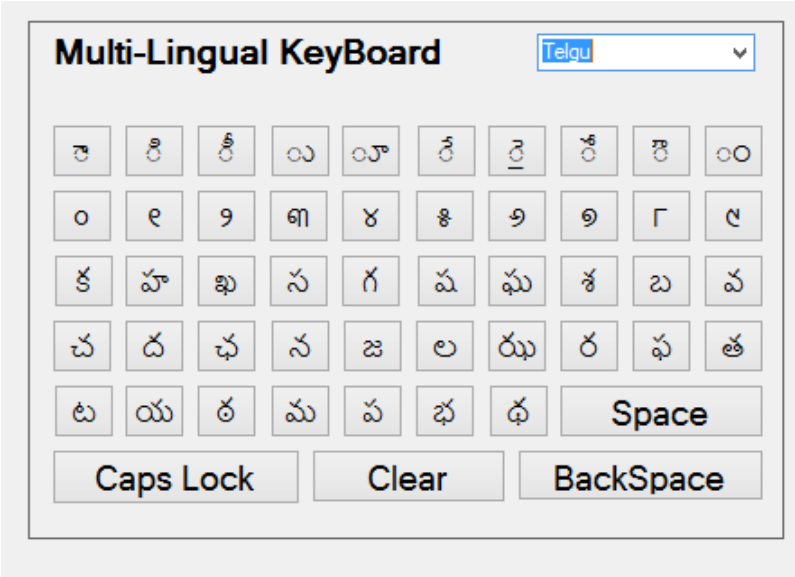

Figure 3.4: Virtual Keyboard - Telgu

Password Length	No of alphabets	No of passwords can be formed	Time Taken (if a computer computes 1 Billion searches per second)
4	10	10,000	1 µs
4	62	456976	14.7 ms
4	260	4569760000	4.56 s
6	10	1,000,000	1 ms
6	62	56800235584	56.8s
6	260	308915776000000	85.80 hrs.
8	10	100,000,000	0.1s
8	62	218340105584896	60.65 hrs.
8	260	208827064576000000000	241697.99 days

Table 3.1

Figure 3.5: Analysis on Brute Force Attack

3.3.3 Shoulder Surfing

Using multilingual keyboard the shoulder surfing will be also reduced up to certain extent. But if we are not randomizing the keyboard every time then the multilingual keyboard will not be very effective to the shoulder surfing. But if we will randomize the key pattern of multilingual keyboard then it will have a better resistance against shoulder surfing.

3.3.4 Key Stroke Dynamics

The main advantage of virtual keyboard is it provides a better resistance against keystroke logging. Using virtual keyboard the key logger or any kind of key stroke based attacks can be avoided.

Chapter 4

Hybrid Authentication Scheme

4.1 About the scheme

Graphical passwords are easy to remember, but they are vulnerable to shoulder surfing. On the other side textual passwords they have many drawbacks but they are simple to implement and use. We are presenting a hybrid technique which is mixture of Textual password, Recognition based graphical password and Recall based Graphical Password. We are implementing the graphical password with the "Stroke based Textual password scheme"[5]. In graphical password we select some point called Point Of Interests during Registration Process. At the time of authentication the user selects the point in the same order as they were chosen in the registration phase. So they are vulnerable to shoulder surfing to a very large extent. In stroke based textual scheme, during registration phase there will be a grid with points and we select a pattern from that grid points. At the time of authentication, the grid points shows either 0 or 1. And every time the different grid comes to the user. The user has to concentrate only on the pattern he had chosen. This is done to provide ambiguity to the attacker. The user has to enter the value of grid points according to the pattern he had selected during Registration phase. This scheme is a good scheme, and provides a better security for the shoulder surfing, but the problem is the pattern selected is static, if the attacker knows what the pattern is, then for him it is very easy. And during the registration phase the attacker can know the pattern.
So we have merged this scheme with graphical password scheme to provide dynamicity

to the pattern selected. At the time of registration user will select a picture, and chose some points on it and for each point he will select a pattern. Now, during Authentication phase the user will select the point in any order, and according to the point selected he will select the pattern by writing 0 and 1 in the textbox. The grid values will change every time so it provides a better resistance to shoulder surfing.

4.2 Implementation

4.2.1 Registration Process

The detailed registration process is shown in figure 4.1

- Browse the image as shown in fig 4.2
- Select first point and corresponding pattern for that as shown in fig 4.3
- Select second point and corresponding pattern as shown in fig 4.4
- Select third point and corresponding pattern as shown in fig 4.5
- Click Ok button

4.2.2 Authentication Process

The detailed authentication process is shown in fig 4.6

- Give user name and select "GO", the corresponding picture will appear.
- Select 3 points in any order, in this picture we have selected p3 - P1 - p2 as in fig 4.7
- According to the order of points selected fill the text box with input string as shown in fig 4.8

Pattern[p3] = 10001, Pattern[p1] = 10011, and pattern[p2] = 101 So textbox will contain 10001 + 10011 + 101 = 10001 10011 101 Note: + is concatenation operator, and pattern[p] means pattern corresponding to point P

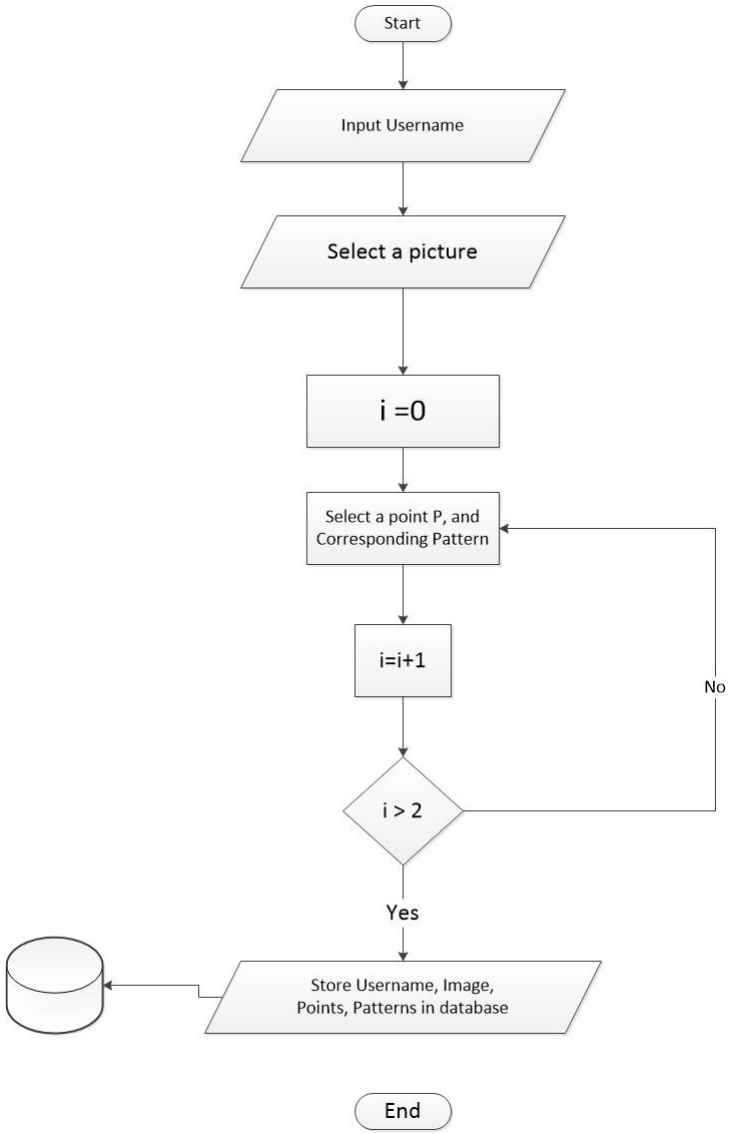

Figure 4.1: Registration Process - Hybrid Password Scheme

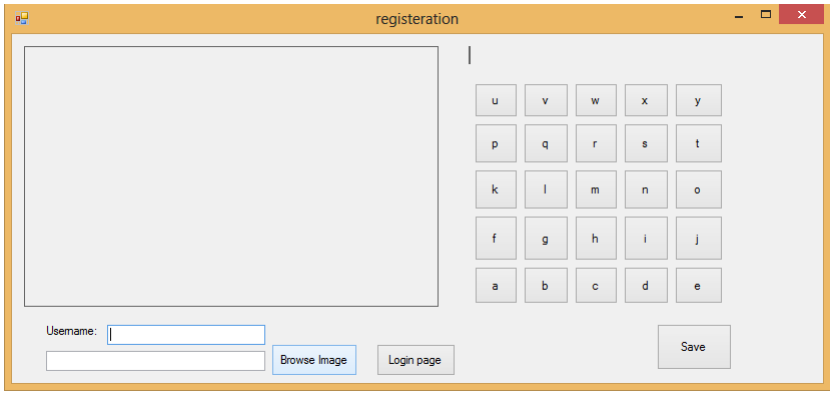

Figure 4.2: Registration process step-1

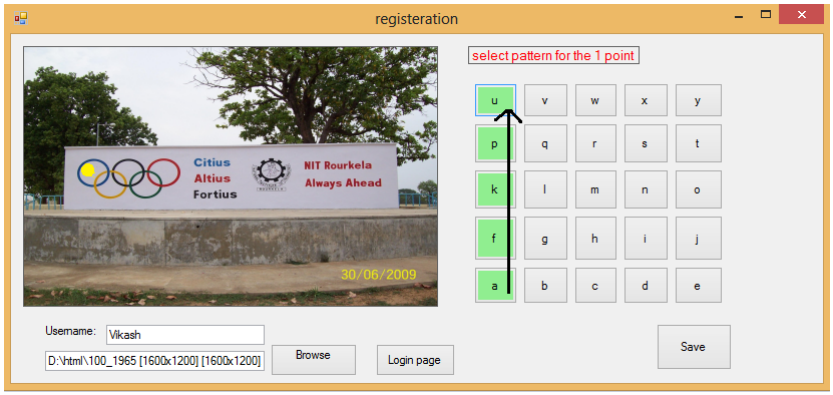

Figure 4.3: Registration process step-2

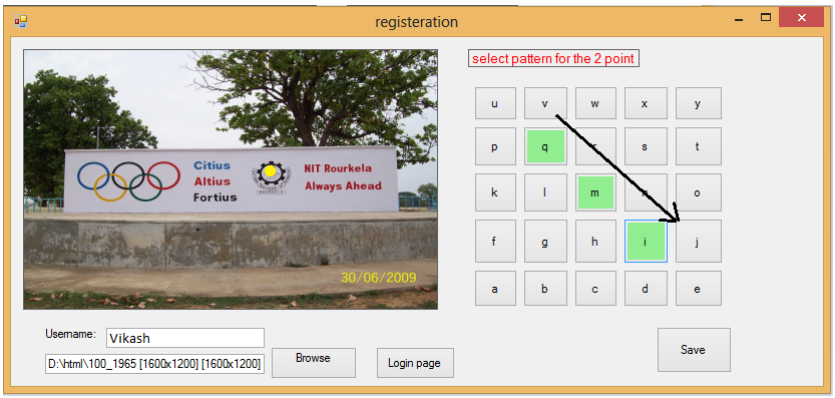

Figure 4.4: Registration process step-3

Figure 4.5: Registration process step-4

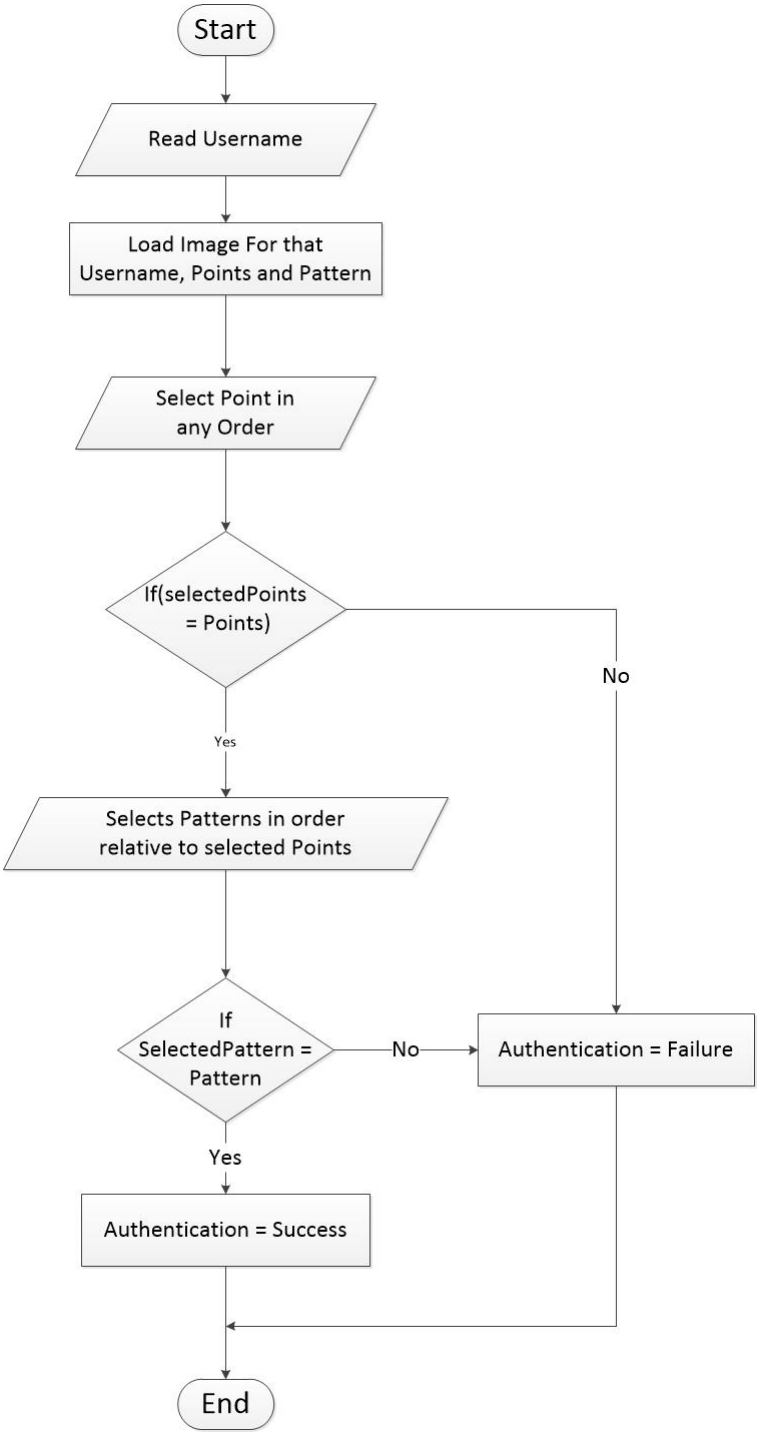

Figure 4.6: Authentication Process - Hybrid Password Scheme

Figure 4.7: Authentication Process step - 2

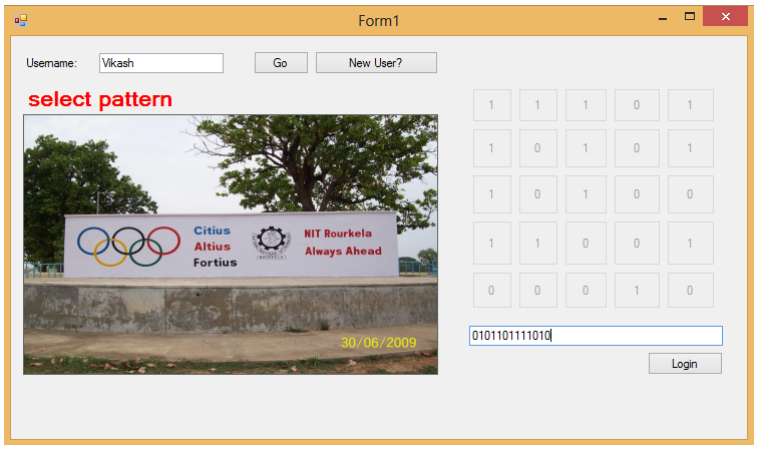

Figure 4.8: Authentication Process step - 2

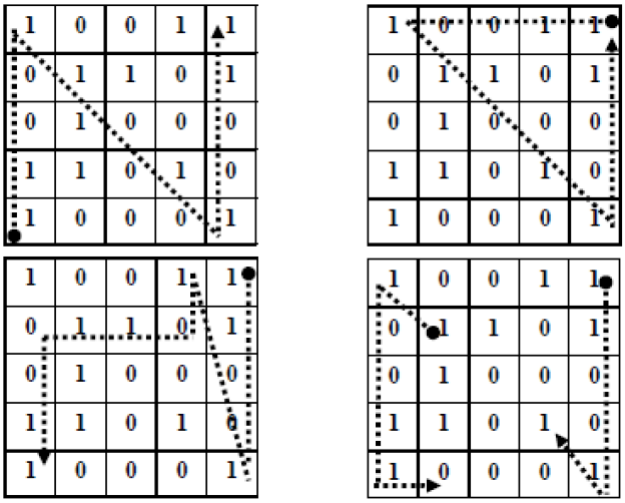

Figure 4.9: Ambiguity in pattern for same input string

If next time we will select the point in same order, the grid values will be different

Pattern [p3] = 01011, Pattern [p1] = 01111, and pattern [p2] = 010 So textbox will contain 01011 + 01111 + 010 = 0101101111010

4.3 Analysis

4.3.1 Shoulder Surfing

This scheme is highly resistive to shoulder surfing. At authentication step the grid values are randomly generated so every time new instance of the interface is created. In addition to that the password is to be entered in a textbox rather than select and click the grid values. And the pattern is dynamic in nature, so it is very difficult to observe. Addition to that, we are using only 0 and 1 in the grid to show the pattern. This provides ambiguity. We can see that for the input string 1100110110011 and with the following grid there may be many patterns as shown in fig 4.9. So this scheme is much stronger and much secure against shoulder surfing.

4.3.2 Eavesdropping

For the same input string there can be different pattern and every time the interface will be changed with new grid values so it will be difficult for the intruder to detect.

The use of graphical password makes the password more dynamic. So the password can be changed by user choice all the time, so pattern can be changed. One can imagine, by input string if a static pattern is difficult to detect then for dynamic pattern it will be worse for the attacker.

4.3.3 Guessing

We have used only two alphabets for the grid values, but if the length of the password is 10 then the possibility of guessing or the effectiveness of random clicking will be 1/210 = 0.0009765625. And if the length of the input string is not known that is exact pattern is not known then this probability will become more less. And security level can be increased by using 3 values at grid positions. But no of alphabets to be used in grid values should be such that it should provide confusion and ambiguity to the attacker.

4.3.4 Brute Force Attack

If the length of the input string that is composed of 0s and 1s is 10 then there may be 210 types of passwords, which seems easy to attack by brute force attack, but the collaboration of pattern with picture and ordering of the points to be selected will provide an effective resistant to the brute force attack also.

4.4 Drawbacks

- This scheme has quite a lengthy login process. So it cant be used everywhere. Some selective application only should have it.
- The registration process is more vulnerable to shoulder surfing. If the attacker notices the points on the image and corresponding patterns then it will be easy for him to detect. Or he can simply apply brute force mechanism.
- Not very simple so there is great chance of mistake for the new users.

Chapter 5

Conclusions

We have discussed several Authentication methods. Our main focus was to protect our system and password from shoulder surfing, eavesdropping, guessing, and stealing of password, brute force attacks and dictionary attacks. Our main focus was on traditional attacks like shoulder surfing, eavesdropping and guessing.

Our 1st scheme Varying Password Scheme provides much security to the eavesdropping and guessing. It was an approach which can be used to use a weaker password in unsafe environment like in public places more effectively. 2nd Scheme was implementation of multilingual virtual keyboard to avoid key stroke dynamics, and to increase the better security against eavesdropping and guessing. And it also provides a much better resistance to brute force attacks by extending the alphabets used.

3rd scheme is a hybrid scheme developed by collaboration of three schemes: textual password, recognition based graphical password and recall based graphical password. All three schemes support each other and use ones advantage to overcome the drawback of another.

Bibliography

[1] Sadiq Almuairfi, Prakash Veeraraghavan, and Naveen Chilamkurti. A novel image-based implicit password authentication system (ipas) for mobile and non-mobile devices. *Mathematical and Computer Modelling*, (0):–, 2012.

[2] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63(12):102 – 127, 2005. ¡ce:title¿HCI research in privacy and security¡/ce:title¿.

[3] M. Shahid and M.A. Qadeer. Novel scheme for securing passwords. In *Digital Ecosystems and Technologies, 2009. DEST '09. 3rd IEEE International Conference on*, pages 223–227, 2009.

[4] A. Almulhem. A graphical password authentication system. In *Internet Security (WorldCIS), 2011 World Congress on*, pages 223–225, 2011.

[5] Ziran Zheng, Xiyu Liu, Lizi Yin, and Zhaocheng Liu. A stroke-based textual password authentication scheme. In *Proceedings of the 2009 First International Workshop on Education Technology and Computer Science - Volume 03*, ETCS '09, pages 90–95, Washington, DC, USA, 2009. IEEE Computer Society.